Detailed Action

This Office Action is response to the application (10/528284) filed on 12/18/2009.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 34-37 rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. More specifically, the applicant fails to sufficiently point out or describe the term "*change in user identification… which further is changing the user identification until the changed user identification matches an authorized user identification.*"

The specification of this application under examination does not contain subject matter to implement limitations, as cited in the following claims.

Claim 34 recites newly presented claim limitation "change in user identification which is further recite changing the user identification until the changed user identification matches an authorized user identification.".

Also, it is not apparent how "change in user identification" is determined. Examiner has reviewed the specification of this application under examination (and OCR whole document) and could not find support for the additional limitations as claimed.

Examiner is interpreting this limitation as "serially or multiple times delivery of the electronic mail" for the purpose of this office action.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 9-16, 25-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Fleming**. US Patent No. **6,249,805** in view of **Sundsted** U.S. Patent No. **US 5,999,967.**

Regarding claim 9, Fleming teaches wherein a method to automatically handle undesired electronic mail (e-mail) in communication networks at the receiver, the method comprising:

automatically comparing the sender address accompanying an incoming e-mail to an electronically accessed list of authorized sender addresses assigned to the receiver **(Fig. 1, unit 106 – authorization component)**; and then

storing the e-mail in a mailbox MB of the recipient **(Fig. 2, unit 205 – store selected Email in inbox folder)**, wherein the only e-mails transferred to the receiver's mailbox are those that had clearly been sent by authorized senders **(Fig. 2, unit 204 – retrieved ID in authorized list)**.

With respect to claim 9, Fleming teaches the invention set forth above except for the claimed "*in combination with:*

performing an analysis to see if there is serial, incremental user identification occurring so that conclusions can be drawn concerning automatic attempts at breaking into the e-mail system."

Sundsted teaches that is well known to utilize filtering the receiving emails in combination with performing an analysis to see if there is serial, incremental user identification occurring so that conclusions can be drawn concerning automatic attempts at breaking into the e-mail system **(Fig. 3A, unit 23 – Analysis Module; Fig. 4, col. 7, lines 50-67; col. 8, lines 17-25)**.

Thus, the manner of enhancing method for filtering unauthorized electronic mail messages that are sent by senders to a user where the system includes a list of the identifications of the senders who are authorized to send an electronic mail message to the user. In addition, the method is used in a system for reducing or eliminating the amount of junk electronic mail in the electronic mail system by Sundsted. Accordingly, one of ordinary skill in the art would have been capable of applying this known "improvement" technique in the same manner to the prior art Fleming and the results

would have been predictable to one of ordinary skill in the art, namely, one skilled in the art would have readily recognized that advantages based on the teachings of Sundsted.

Regarding claim 10, Fleming and Sundsted together taught the method according as in claim 9 above. Fleming further teaches wherein there are two logically or physically, or both, separate mailboxes, said mailbox MB **(inbox folder)** and a junk mailbox JMB **(Junk Mail folder)**, wherein the e-mail server sends to the JMB mailbox all incoming e-mails that indeed have the subscriber's correct recipient address but are not contained in the sender list on the receiving side **(If the retrieved ID does not match, than the authorization component stores the intercepted electronic mail message in a pre-designated location, such as a Junk Mail folder – Col. 4, lines 24-27)**, thus making them available for further processing selectively by the internet service provider, the administrative authorities, and by the recipient **(periodically, the user can view the Junk mail folder to delete or read (means further processing) the electronic messages that we designed as junk – Col. 4, lines 34-36)**.

Regarding claims 11-12, Fleming and Sundsted together taught the method according as in claim 9 above. Fleming further teaches wherein the incoming e-mails are selectively put through an automatic handling and analysis process **(The authorization component intercepts electronic mail messages that are sent to a user before they are placed in the user's Inbox folder—Col. 4, lines 15-17)**, which can be selectively configured by the recipient and by the ISP **(forwards the electronic mail**

message to the recipient via a communications mechanism such as a local area network or the Internet – Col. 1, lines 18-20), selectively in the e-mail server, in a comparison device **(various computer systems – Col. 1, lines 35)**, and in at least one of the mailboxes **(Inbox folder or Junk Mail folder)**, said process initiated and configured either on a case-by-case basis or permanently **(Fig. 3)**.

Sundsted further teaches wherein the incoming e-mails are selectively put through an automatic handling and analysis process, which can be selectively configured by the recipient and by the ISP, selectively in the e-mail server, in a comparison device, and in at least one of the mailboxes, said process initiated and configured either on a case-by-case basis or permanently **(Procmail – Col. 1, lines 30-41).**

Claims 13-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Fleming**. US Patent No. **6,249,805** in view of **Sundsted** U.S. Patent No. **US 5,999,967** further in view of **Shipp** US Patent App. No. **US 20040054498**.

Regarding claims 13-16, Fleming and Sundsted together taught the method according as in claim 9 above. However, Fleming and Sundsted are silent in term "*wherein all executable programs sent as attachments to e-mails are automatically separated*" **Shipp** teaches that it is well known to have system wherein when executable programs are sent as attachments to e-mails, all said executable programs are automatically separated in the JMB **(the attachment must contain some**

executable element to be viewed as a potential threat ….– [0104-0105; 0134-0137]).

Thus, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Fleming's and Sundsted's invention by a component normally considered as an attachment: These may be directly executable, such as an EXE file. They may contain embedded executable code, such as a Microsoft Word document containing a macro. They may contain archive file or other container files, which themselves may contain other dangerous components. For instance, a ZIP file may contain an executable. In addition, the system is capable of being toggled into a mode where it views all attachments as a potential threat disposing of the infected emails without sending them to their addressed recipients. Holding them in temporary storage "***here is same JMB***" and notifying the addressee by email that an infected message has been intercepted and is being held for a period for their retrieval, should they wish, otherwise it will be deleted

Regarding claims 25-28, Fleming and Sundsted together taught the method according as in claim 9 above. Fleming further teaches wherein the contents of the JMB can be cyclically deleted at specific time intervals **(Periodically, the user can view the Junk Mail folder to delete or read the electronic mail messages that were designated as junk – Col. 4, lines 33-36)**.

Claims 17-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Fleming**. US Patent No. **6,249,805** in view of **Sundsted** U.S. Patent No. **US 5,999,967** further in view of **Weeks** US Patent App. No. **US 20040054733**.

Regarding claims 17- 20, Fleming and Sundsted together taught the method according as in claim 9 above. However, Fleming and Sundstead are silent in terms of "wherein if an undesired e-mail is received, discontinuation requests, or cease and desist demands, can be generated automatically and delivered to the sender".
Weeks teaches that it is well known to have a method "wherein if an undesired e-mail is received, discontinuation requests, or cease and desist demands, can be generated automatically and delivered to the sender" **(FIGS. 4-9 provide flow diagrams illustrating exemplary processes implemented in the e-mail management system 10 of FIG. 1. – [0011-0016])** in order to make the system more efficient and that prevent delivery of unsolicited e-mail are known.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Fleming's and Sundsted's invention by utilizing a system wherein after reviewing the e-mail stored in the inbox folder 102, the user may determine that an e-mail is an unsolicited e-mail and thus may desire to prevent delivery of further email from the sender of the unsolicited e-mail. To do so, the user selects the unsolicited e-mail and places it in the e-mail stop folder 104. The system 10 then automatically generates stop data 106 based on the unsolicited e-mail stored in the e-mail stop folder 104 to prevent delivery of any further e-mail sent to the user address

from the sender, as taught by Weeks [0019].

Claims 21-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Fleming**. US Patent No. **6,249,805** in view of **Sundsted** U.S. Patent No. **US 5,999,967** further in view of **Lalonde** US Patent No. **US 7,072,944** further in view of **Shipp** US Patent App. No. **US 20040054498**

Regarding claims 21-24, Fleming and Sundsted together taught the method according as in claim 9 above. However Fleming and Sundsted are silent in terms of "*wherein virus checks of the e-mail can be carried out selectively at an established time of day or each time a message arrives.*"

Lalonde teaches that it is well known to have "wherein virus checks of the e-mail can be carried out selectively at an established time of day or each time a message arrives" **(Fig. 9, unit 174 – virus check)**.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Fleming's and Sundsted's invention by utilizing virus system in which it solves the major problems of ensuring that the emails are handled in an efficient and timely manner in the email engine. The application is typically provided on a client machine (e.g. PCs) and communicates with a mail server so that, when the client machine receives email from the mail server, the client plug-in authenticates the email as described herein. Thus, each time the virus protection application checks an

email for a virus, it also authenticates the email to obtain an authentication indicator which informs a user of the likelihood of the email being spoofed (as taught by Lalonde).

Claim 29-37 list all the same elements of **claim 9-17, 21, 25**, but in storage system rather than method form. Therefore, the supporting rationale of the rejection to **claim 9-17, 21, 25** applies equally as well to **claim 29-37**.

Response to Arguments

Applicant's arguments filed on 12/18/2009 have been fully considered but they are not persuasive.

Applicant Argument:

The analyses performed by Sundsted's Analysis Module 23 are quire different from the analysis recited in the last paragraph of claim 9, which requires (a) that the analysis is to see if there is serial, incremental *user identification* occurring, and (b) that the occurrence of serial, incremental *user identification* enables conclusions to be drawn concerning automatic attempts at breaking into the e-mail system.

Examiner Response:

With respect to Applicant arguments on page 7-13 of the remark, it must be noted that "Claims are to be given their broadest reasonable interpretation during prosecution, and the scope of a claim cannot be narrowed by reading disclosed limitations into the claim. *See In re Morris*, 127 F.3d 1048, 1054, 44 USPQ2D 1023,

1027 (Fed. Cir. 1997); In re Zletz, 893 F.2d 319, 321, 13 USPQ2D 1320, 1322 (Fed. Cir. 1989); *In re Prater*, 415 F.2d 1393, 1404, 162 USPQ 541,550 (CCPA 1969)."

Sundsted discloses an Analysis Module 23 which decides whether to accept, reject, or otherwise handle electronic mail based on the value of its electronic stamp. In FIG. 4, the electronic stamp comprises the following fields: e.g., a Serial Number Field 40 where the Serial Number Field holds the serial number of the electronic stamp. This number is issued by the sending system. According to Sundsted, a serial number must never be reissued. The simplest serial number generator is a counter that is incremented for each electronic stamp generated.

For example, in step (g) Analysis Module 23 reads the serial number from Serial Number Field 40. It then checks History Log 25 to see if this electronic stamp has been received before. If the electronic stamp is found in History Log 25, this is a good indication that the electronic mail has been delivered multiple times "*here it's considered the electronic mail has been delivered serially*" due to malicious intent. In this case, the associated electronic mail should be rejected (*here is the same as that the occurrence of serial, incremental user identification enables conclusions to be drawn concerning automatic attempts at breaking into the e-mail system* (col. 8, lines 17-25)). Therefore, Examiner maintains the rejections.

In addition, the applicant specification dose not further discloses and support an interpretation of the terms serial/incremental user ID, therefore it is not clear what is it referring to? (e.g., is it the same as when a user with a unique ID (e.g., email address) sending emails repeatedly to break the system; or is it the same as when a user with a

different domains (e.g., email addresses) sending emails repeatedly to break the system?)

Thus, since the applicant specification is silent in terms further definition of serial/incremental user ID, in this case, the above term is defined based on a broadest reasonable interoperation to enable one of the ordinary skill in the art, where the serial is directed to "one event after another" based on the Newton's dictionary.

Also must be noted is "In addition, the law of anticipation does not require that a reference "teach" what an appellant's disclosure teaches. Assuming that reference is properly "prior art," it is only necessary that the claims "read on" something disclosed in the reference, i.e., all limitations of the claim are found in the reference, or "fully met" by it. *Kalman v. Kimberly-Clark Corp.*, 71 3 F.2d 760, 772, 21 8 USPQ 781,789 (Fed. Cir. 1983).

Therefore, based on a broadest reasonable interoperation, Sundsted invention dose disclose that applicant claim limitation by utilizing "e.g., the simplest serial number generator, which is a counter and that is incremented for each electronic stamp generated " (col. 7, Lines 1-5). Therefore, Examiner maintains the rejection.

Applicant Argument:

This assertion by the Examiner is not based upon a reasonable interpretation of the plain language of the terms of the claims and is not consistent with the Specification of the present application for at least the following reasons:

• Sundsted's Analysis Module 23 does not see if serial, incremental user identification is

occurring, as required by the plain language of the last paragraph of claim 9.

Examiner Response

With respect to Applicant arguments on page 7-13 of the remark, it must be noted that "Claims are to be given their broadest reasonable interpretation during prosecution, and the scope of a claim cannot be narrowed by reading disclosed limitations into the claim. *See In re Morris*, 127 F.3d 1048, 1054, 44 USPQ2D 1023, 1027 (Fed. Cir. 1997); In re Zletz, 893 F.2d 319, 321, 13 USPQ2D 1320, 1322 (Fed. Cir. 1989); *In re Prater*, 415 F.2d 1393, 1404, 162 USPQ 541,550 (CCPA 1969)."

Sundsted discloses an Analysis Module 23 which decides whether to accept, reject, or otherwise handle electronic mail based on the value of its electronic stamp. In FIG. 4, the electronic stamp comprises the following fields: e.g., a Serial Number Field 40 where the Serial Number Field holds the serial number of the electronic stamp. This number is issued by the sending system. According to Sundsted, a serial number must never be reissued. The simplest serial number generator is a counter that is incremented for each electronic stamp generated.

For example, in step (g) Analysis Module 23 reads the serial number from Serial Number Field 40. It then checks History Log 25 to see if this electronic stamp has been received before. If the electronic stamp is found in History Log 25, this is a good indication that the electronic mail has been delivered multiple times "*here it's considered the electronic mail has been delivered serially*" due to malicious intent. In this case, the associated electronic mail should be rejected (*here is the same as that the occurrence*

of serial, incremental user identification enables conclusions to be drawn concerning automatic attempts at breaking into the e-mail system (col. 8, lines 17-25)). Therefore, Examiner maintains the rejections.

In addition, the applicant specification dose not further discloses and support an interpretation of the terms serial/incremental user ID, therefore it is not clear what is it referring to? (e.g., is it the same as when a user with a unique ID (e.g., email address) sending emails repeatedly to break the system; or is it the same as when a user with a different domains (e.g., email addresses) sending emails repeatedly to break the system?)

Thus, since the applicant specification is silent in terms further definition of serial/incremental user ID, in this case, the above term is defined based on a broadest reasonable interoperation to enable one of the ordinary skill in the art, where the serial is directed to "one event after another" based on the Newton's dictionary.

Also must be noted is "In addition, the law of anticipation does not require that a reference "teach" what an appellant's disclosure teaches. Assuming that reference is properly "prior art," it is only necessary that the claims "read on" something disclosed in the reference, i.e., all limitations of the claim are found in the reference, or "fully met" by it. *Kalman v. Kimberly-Clark Corp.*, 71 3 F.2d 760, 772, 21 8 USPQ 781,789 (Fed. Cir. 1983).

Therefore, based on a broadest reasonable interoperation, Sundsted invention dose disclose that applicant claim limitation by utilizing "e.g., the simplest serial number

generator, which is a counter and that is incremented for each electronic stamp generated" (col. 7, Lines 1-5). Therefore, Examiner maintains the rejection.

Applicant Argument:

Such an occurrence of serial, incremental *electronic stamp serial number identification* does *not* enable a conclusion to be drawn concerning automatic attempts at breaking into the e-mail system, as required by the last paragraph of claim 9.

Examiner Response

With respect to Applicant arguments on page 7-13 of the remark, it must be noted that "Claims are to be given their broadest reasonable interpretation during prosecution, and the scope of a claim cannot be narrowed by reading disclosed limitations into the claim. *See In re Morris*, 127 F.3d 1048, 1054, 44 USPQ2D 1023, 1027 (Fed. Cir. 1997); In re Zletz, 893 F.2d 319, 321, 13 USPQ2D 1320, 1322 (Fed. Cir. 1989); *In re Prater*, 415 F.2d 1393, 1404, 162 USPQ 541,550 (CCPA 1969)."

Sundsted discloses an Analysis Module 23 which decides whether to accept, reject, or otherwise handle electronic mail based on the value of its electronic stamp. In FIG. 4, the electronic stamp comprises the following fields: e.g., a Serial Number Field 40 where the Serial Number Field holds the serial number of the electronic stamp. This number is issued by the sending system. According to Sundsted, a serial number must

never be reissued. The simplest serial number generator is a counter that is incremented for each electronic stamp generated.

For example, in step (g) Analysis Module 23 reads the serial number from Serial Number Field 40. It then checks History Log 25 to see if this electronic stamp has been received before. If the electronic stamp is found in History Log 25, this is a good indication that the electronic mail has been delivered multiple times "*here it's considered the electronic mail has been delivered serially*" due to malicious intent. In this case, the associated electronic mail should be rejected (*here is the same as that the occurrence of serial, incremental user identification enables conclusions to be drawn concerning automatic attempts at breaking into the e-mail system* (col. 8, lines 17-25)). Therefore, Examiner maintains the rejections.

In addition, the applicant specification dose not further discloses and support an interpretation of the terms serial/incremental user ID, therefore it is not clear what is it referring to? (e.g., is it the same as when a user with a unique ID (e.g., email address) sending emails repeatedly to break the system; or is it the same as when a user with a different domains (e.g., email addresses) sending emails repeatedly to break the system?)

Thus, since the applicant specification is silent in terms further definition of serial/incremental user ID, in this case, the above term is defined based on a broadest reasonable interoperation to enable one of the ordinary skill in the art, where the serial is directed to "one event after another" based on the Newton's dictionary.

Also must be noted is "In addition, the law of anticipation does not require that a reference "teach" what an appellant's disclosure teaches. Assuming that reference is properly "prior art," it is only necessary that the claims "read on" something disclosed in the reference, i.e., all limitations of the claim are found in the reference, or "fully met" by it. *Kalman v. Kimberly-Clark Corp.*, 71 3 F.2d 760, 772, 21 8 USPQ 781,789 (Fed. Cir. 1983). Therefore, Examiner maintains the rejection.

Applicant Argument:

It must be concluded that Sundsted does not teach either (a) an analysis to see if serial, incremental user identification is occurring or (b) that it is when serial, incremental user identification is occurring that a conclusion can be drawn that there is an automatic attempt at breaking into the e-mail system, as required by the last paragraph of claim 9.

Examiner Response

With respect to Applicant arguments on page 7-13 of the remark, it must be noted that "Claims are to be given their broadest reasonable interpretation during prosecution, and the scope of a claim cannot be narrowed by reading disclosed limitations into the claim. *See In re Morris*, 127 F.3d 1048, 1054, 44 USPQ2D 1023, 1027 (Fed. Cir. 1997); In re Zletz, 893 F.2d 319, 321, 13 USPQ2D 1320, 1322 (Fed. Cir. 1989); *In re Prater*, 415 F.2d 1393, 1404, 162 USPQ 541,550 (CCPA 1969)."

Sundsted discloses an Analysis Module 23 which decides whether to accept, reject, or otherwise handle electronic mail based on the value of its electronic stamp. In FIG. 4, the electronic stamp comprises the following fields: e.g., a Serial Number Field 40 where the Serial Number Field holds the serial number of the electronic stamp. This number is issued by the sending system. According to Sundsted, a serial number must never be reissued. The simplest serial number generator is a counter that is incremented for each electronic stamp generated.

For example, in step (g) Analysis Module 23 reads the serial number from Serial Number Field 40. It then checks History Log 25 to see if this electronic stamp has been received before. If the electronic stamp is found in History Log 25, this is a good indication that the electronic mail has been delivered multiple times "*here it's considered the electronic mail has been delivered serially*" due to malicious intent. In this case, the associated electronic mail should be rejected (*here is the same as that the occurrence of serial, incremental user identification enables conclusions to be drawn concerning automatic attempts at breaking into the e-mail system* (col. 8, lines 17-25)). Therefore, Examiner maintains the rejections.

In addition, the applicant specification dose not further discloses and support an interpretation of the terms serial/incremental user ID, therefore it is not clear what is it referring to? (e.g., is it the same as when a user with a unique ID (e.g., email address) sending emails repeatedly to break the system; or is it the same as when a user with a different domains (e.g., email addresses) sending emails repeatedly to break the system?)

Thus, since the applicant specification is silent in terms further definition of serial/incremental user ID, in this case, the above term is defined based on a broadest reasonable interoperation to enable one of the ordinary skill in the art, where the serial is directed to "one event after another" based on the Newton's dictionary.

Also must be noted is "In addition, the law of anticipation does not require that a reference "teach" what an appellant's disclosure teaches. Assuming that reference is properly "prior art," it is only necessary that the claims "read on" something disclosed in the reference, i.e., all limitations of the claim are found in the reference, or "fully met" by it. *Kalman v. Kimberly-Clark Corp.*, 71 3 F.2d 760, 772, 21 8 USPQ 781,789 (Fed. Cir. 1983).

Therefore, based on a broadest reasonable interoperation, Sundsted invention dose disclose that applicant claim limitation by utilizing "e.g., the simplest serial number generator, which is a counter and that is incremented for each electronic stamp generated " (col. 7, Lines 1-5). Therefore, Examiner maintains the rejection.

Applicant Argument:

However, Shipp does *not* teach or suggest that *all* attached executable programs sent as attachments to e-mails are automatically separated, as required by claims 13-16.

Shipp's only teaching of an executable program being separated from an email is in paragraph 0137. This teaching does not suggest that *all* said executable programs are *automatically* separated, as required by each of claims 13-16.

Examiner Response

With respect to Applicant argument, Shipp further discloses a component normally considered as an attachment: These may be directly executable, such as an EXE file. They may contain embedded executable code, such as a Microsoft Word document containing a macro. They may contain archive file or other container files, which themselves may contain other dangerous components. For instance, a ZIP file may contain an executable – [0104].

Normally, the attachment must contain some executable element to be viewed as a potential threat. However, the system is capable of being toggled into a mode where it views all attachments as a potential threat – [0105].

This is to cater for two possibilities such as: A document, such as a jpg picture, may contain illegal formatting that crashes the application used to view the attachment. This can cause either a denial of service attack, or an exploit which can cause a security breach or spread a virus – [0106].

Shipp further disclosing the term stopper 25, which takes signatures from the searcher 24. The signature identifies characteristics of emails which must be stopped.

On receiving the signature, all future matching emails are treated as viruses, and stopped. Obviously, the stopping action can take a number of forms, including:

Disposing of the infected emails without sending them to their addressed recipients (here is same as that *all* attached executable programs sent as attachments to e-mails are automatically separated).

Holding them in temporary storage and notifying the addressee by email that an infected message has been intercepted and is being held for a period for their retrieval, should they wish, otherwise it will be deleted (here is same as that *all* attached executable programs sent as attachments to e-mails are automatically separated).

Disinfecting the email by removing the virus threat by any suitable means; for example if the virus is an executable attachment, it can be detached or disarmed before forwarding the email to its addressees. The email may be modified by the inclusion of a text message saying that the email has been disinfected (here is same as that *all* attached executable programs sent as attachments to e-mails are automatically separated) - [0133-0137].

In addition, Applicant fails to disclose in the claims 13-16, further steps, in the time, while the separation step is taken place, is it separating only the EXE. attachments from the emails and than forward the received email with out the attachments to their recipients, Or the system will separates together both the emails along with its executable file attachments.

Furthermore, the Applicant failed to provide further supports on the specification as well that how to enable an ordinary skill in the art in terms of the above claim limitation. In other word, there is not such disclosure in specification to determine or perform that all attached executable programs sent as attachments to e-mails are automatically separated only or along with its emails. However, Shipp further discloses the above claim limitation, therefore, Examiner maintains the rejections.

Conclusion

Applicant's argument filed on 12/18/2009, have been fully considered but they are not persuasive. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action. Any inquiry concerning this communication or earlier communications from the examiner should be directed to SULAIMAN NOORISTANY whose telephone number is (571)270-1929. The examiner can normally

be reached on Monday Through Friday 9:30 am to 5:00 pm EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffery Pwu can be reached on 571-272-6798. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Sulaiman Nooristany 03/21/2010

/Jeffrey Pwu/

Supervisory Patent Examiner, Art Unit 2446